23 May 2006

INFORMATION PAPER

SUBJECT: Department of Veterans Affairs Lost Personal Data

1. **Purpose**. To provide information and guidance to those veterans and their families who are potential victims of identity theft.

2. **Facts**.

a. **Background**. In May 2006, the Department of Veterans Affairs (VA) discovered that personal information for over 26 million veterans and their spouses was stolen during a robbery at the home of a VA data analyst. The analyst took the information home in violation of VA policy and is currently on administrative leave pending the result of the investigation. The stolen information includes names, social security numbers, disability ratings and dates of birth of veterans who have retired since 1972. No medical records were stolen.

b. **Investigation**. The FBI and the VA are conducting a full-scale investigation into this matter. Authorities believe it is unlikely the perpetrators targeted the personal data or are aware they have this sensitive information. To date, authorities have not detected any suspicious activity connected with the lost data. In an effort to fully inform those potentially affected, the VA will send out individual notification letters to veterans and their families.

c. **Reporting Suspicious Activities**. If you receive a notification letter from the VA, it is because your personal information was stolen. You should be especially vigilant for any signs that other people may have attempted to exploit your personal information. While there is no evidence yet that any missing data has been used illegally, all veterans should carefully monitor bank statements, credit card statements and any other statements relating to recent financial transactions. If there is any suspicious activity on your statements, you should report it immediately to the financial institution involved and contact the Federal Trade Commission at www.consumer.gov/idtheft or at 1-877-ID-THEFT (438-4338) for further guidance. Such complaints will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for their investigations. You should also contact the local police. Be sure to get a copy of the police report because many creditors require an official report to absolve you of fraudulent debts.

d. **Fraud Alert**. If you receive a notification letter, you should seriously consider placing a fraud alert on your credit files. Initiating a fraud alert would be the most prudent action for most victims, with the exception of those persons who are about to seek a substantial credit line (such as buying a house). A fraud alert stays on a credit file for 90 days and may be extended. The alert tells creditors to contact you before opening any new credit accounts or changing any of your existing accounts. To place a fraud alert, call any one of the three major credit bureaus listed below:

(1) Equifax at 1-800-525-6285 or write to P.O. Box 740250, Atlanta, GA 30374-0250 or visit their website at www.equifax.com.

(2) Experian (formerly TRW) at 1-888-397-3742, or fax at 1-800-301-7196 or write to P.O. Box 1017, Allen, TX 75013 or visit their website at www.experian.com.

(3) Trans Union at 1-800-680-7289 or write to P.O. Box 6790, Fullerton, CA 92634 or visit their website at www.transunion.com.

When you notify one credit bureau, they are required to alert the others. All three credit bureaus will then send credit reports, free of charge, for your review. You should review your credit reports for any suspicious activity regularly for at least eighteen months.

e. **Additional Information**. The Department of Veterans Affairs has established a dedicated toll free telephone number (1-800-FED-INFO) for questions or concerns connected with this loss of data. You can also visit their website at www.firstgov.gov for updates.

CPT Smith/ATJA/4189
Approved by COL Curry, TRADOC SJA